INC-01101-Z3M0

# ALERTA DE SEGURIDAD

CSIRT-RD

Equipo Nacional de Respuestas a Incidentes Cibernéticos del CNCS

FECHA DE PUBLICACIÓN: 19 DE JUNIO 2020



CNCS CENTRO NACIONAL DE CIBERSEGURIDAD REPÚBLICA DOMINICANA

REPÚBLICA DIGITAL

REPÚBLICA DOMINICANA Con la gente y para la gente | MINISTERIO DE LA PRESIDENCIA




# ALERTA DE SEGURIDAD

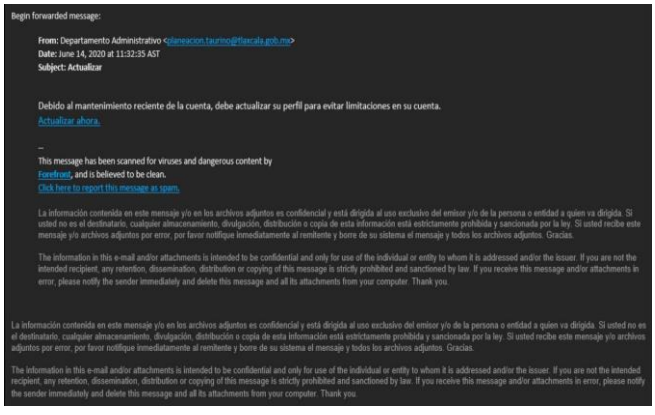
- **ID** INC-01101-Z3M0
- **TLP** Blanco
- **Tipo de incidente Ingeniería** Social
- **Categoría** Robo de Información
- **Fecha de incidente** 14 de junio 2020
- **Fecha de reporte** 15 de junio 2020
- **Nivel de peligrosidad Alto**

# RESUMEN EJECUTIVO

Las organizaciones están expuestas a diferentes amenazas cibernéticas como consecuencia de la utilización de páginas web, aplicaciones móviles, correo electrónico, redes sociales, entre otras. La mayoría de estas amenazas están siendo diseñadas para el robo de información personal o corporativa con el objetivo de crear ataques cibernéticos. Dentro de los métodos comúnmente utilizados se encuentran el uso de correos electrónicos masivos con informaciones erróneas o con links para que el usuario realice acciones que tienen como principal objetivo capturar información o distribuir código malicioso en los equipos de los usuarios.

# DETALLES DE LA ALERTA

A través de una notificación al correo de reportes de incidentes del Equipo Nacional de Respuestas a Incidentes Cibernéticos (CSIRT-RD), se ha identificado una campaña de phishing vía correo electrónico con los asuntos; "**Actualizar"** o **"Plazo de 24 horas"** que invita al usuario acceder a un link para actualizar los datos de su cuenta y poder continuar utilizando el servicio



Begin forwarded message:

**From:** Departamento Administrativo <planeacion.taurino@tlaxcala.gob.mx>
**Date:** June 14, 2020 at 11:32:35 AST
**Subject:** Actualizar

Debido al mantenimiento reciente de la cuenta, debe actualizar su perfil para evitar limitaciones en su cuenta.
Actualizar ahora.

--
This message has been scanned for viruses and dangerous content by
Forefront, and is believed to be clean.
Click here to report this message as spam.

La información contenida en este mensaje y/o en los archivos adjuntos es confidencial y está dirigida al uso exclusivo del emisor y/o de la persona o entidad a quien va dirigida. Si usted no es el destinatario, cualquier almacenamiento, divulgación, distribución o copia de esta información está estrictamente prohibida y sancionada por la ley. Si usted recibe este mensaje y/o archivos adjuntos por error, por favor notifique inmediatamente al remitente y borre de su sistema el mensaje y todos los archivos adjuntos. Gracias.

The information in this e-mail and/or attachments is intended to be confidential and only for use of the individual or entity to whom it is addressed and/or the issuer. If you are not the intended recipient, any retention, dissemination, distribution or copying of this message is strictly prohibited and sanctioned by law. If you receive this message and/or attachments in error, please notify the sender immediately and delete this message and all its attachments from your computer. Thank you.

La información contenida en este mensaje y/o en los archivos adjuntos es confidencial y está dirigida al uso exclusivo del emisor y/o de la persona o entidad a quien va dirigida. Si usted no es el destinatario, cualquier almacenamiento, divulgación, distribución o copia de esta información está estrictamente prohibida y sancionada por la ley. Si usted recibe este mensaje y/o archivos adjuntos por error, por favor notifique inmediatamente al remitente y borre de su sistema el mensaje y todos los archivos adjuntos. Gracias.

The information in this e-mail and/or attachments is intended to be confidential and only for use of the individual or entity to whom it is addressed and/or the issuer. If you are not the intended recipient, any retention, dissemination, distribution or copying of this message is strictly prohibited and sanctioned by law. If you receive this message and/or attachments in error, please notify the sender immediately and delete this message and all its attachments from your computer. Thank you.

Se ha analizado el enlace suministrado en un ambiente controlado y se observa que redirige a un portal donde se solicita introducir las credencias con el fin de capturar la información.

# INDICADORES DE COMPROMISO (IoC)

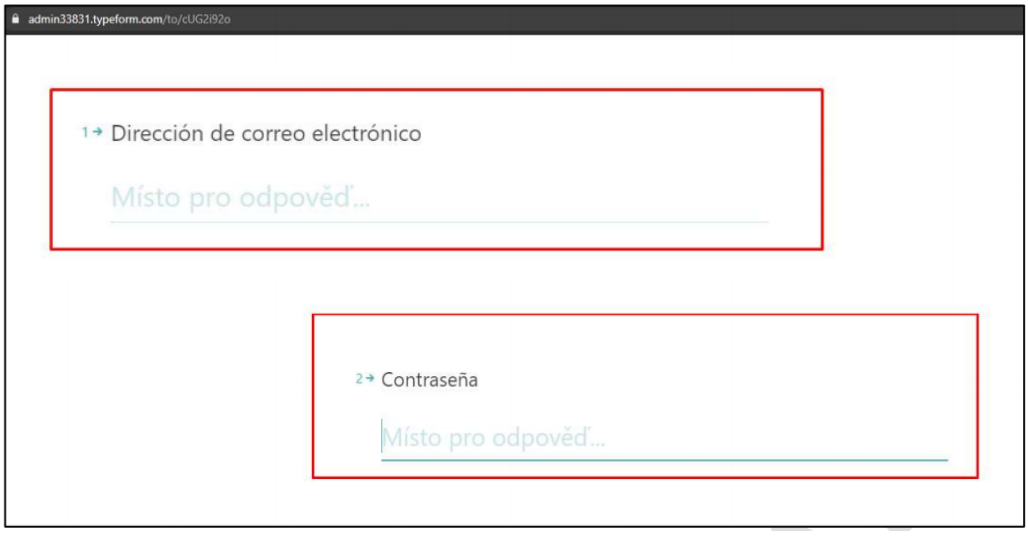
**Remitente**
Planeación[.]taurino@[Tlaxcala].gob.mx
Acastillo[.]ce@[Tlaxcala].gob.mx

**Asunto**
"Actualizar"
"Plazo de 24 horas "

**Conexiones IP**
143[.]204[.]99[.]83
54[.]200[.]147[.]126
52[.]70[.]241[.]23

**Soluciones de DNS**
admin33831[.]typeform[.]com
Api[.]segment[.]io
Cdn[.]segment[.]com
renderer-assets[.]typeform[.]com

**URL**
https:[//]admin33831.typeform[.]com/to/cUG2i92o





1. Realizar el análisis correspondiente para el bloqueo a los indicadores de compromiso expuestos, indicados en este documento.
2. Recomendamos tener precaución al momento de acceder a enlaces suministrados adjuntos vía correo electrónico.
3. Mantener actualizadas las plataformas y sistemas de información.
4. Realizar campañas de concientización periódica a todos los usuarios de la institución.